REMARKS

Claims 1-11 are in the application. By these amendments claims 1-4 are canceled leaving claims 5-11 pending.

Claims 5-11 stand rejected under 35 U.S.C. §102(3) as being anticipated by Buffam (US 6,185,316). This rejection is respectfully traversed on the following grounds.

Buffam relates to a system and method that is primarily directed to self-authentication. The process does permit transmission of some plaintext and ciphertext, however, the main function as shown in Fig. 8 is to authenticate that the claimant (612) is identical to the enrolled user (535). In that depicted embodiment, it uses the enrollee's fingerprint to encrypt information that is stored on a "transient template" (e.g., a magnetic strip or smart card). A claimant presenting the transient template at an authentication station performs a live fingerprint scan (col. 21, line 1). The claimant's newly generated fingerprint is used there to decrypt the transient template. For example, the decryption results in plaintext that is compared with known plaintext to verify that the claimant is the authorized user (col. 10, lines 10-18).

The office action asserts that Buffam anticipates every element of the claimed invention. Applicant respectfully disagrees. Like Buffam, Applicant's invention uses a fingerprint to encrypt information for transmission to a recipient. However, the claimed process of securely communicating the sender's information to the ultimate recipient includes more than mere fingerprint encoding and is thus dramatically different from that of Buffam.

The process of claim 5 calls for obtaining the sender's fingerprint and developing a first encoding key based on that fingerprint; delivering the first encoding key to a third party (key control system); transmitting the encrypted information to the third party and having the third party decrypt the information using the first encoding key. The claimed process further includes having the third party receive a second encoding key developed from the fingerprint of the ultimate receiver of the information; the third party encrypting the information that it had obtained from the sender but using the second encoding key; and transmitting the re-encrypted information to the second party receiver. Finally, the second party receiver uses the second encoding key to decrypt the information that was sent by the third party.

For a claim to be anticipated under section 102, all of the limitations of the claim must be evident from the prior art. Buffam does not teach or suggest the claimed steps involving providing two encoding keys, one each being from the sender and the receiver. Furthermore, Buffam does not disclose that the first encrypted information is decrypted using a first encoding key and encrypted a second time using a second encoding key. The first and second encoding keys are respectively developed from fingerprints of the sender and the receiver. Axiomatically, fingerprints are unique to the individual. Therefore, the claimed process implies that the two encoding keys are different. Buffam nowhere mentions that the transmitted information is to be encoded using a key other than one developed from the fingerprint of the original sender.

Another distinction between Buffam and this claimed invention is that the former process calls for the enrollee-claimant to be present at both the enrolling station where the information transmitted originates and the authentication station where the decoding key is recovered. As recited in the description bridging columns 20 and 21:

> Key Recovery
> Continuing in Fig. 8, the key recovery process, step 610, is presently described. Claimant 612 presents credential 605 to credential sensor 615 contemporaneously with providing a live fingerprint scan from fingerprint sensor 614. Transient template 620 is then extracted from credential 605. (Emphasis added.)

As mentioned, the claimed process calls for the sender and the receiver to provide personalized encoding keys based upon their respective fingerprints to a third party. That party is independent of both the sender and receiver. The third party performs intermediate decryption and encryption services and this obviates the need for the sender to be present at the key recovery station as required by Buffam. Still further, there is no mention in Buffam of three parties to the transmission of the information or of a key control system that is independent of both the sender and the receiver. Buffam thus discloses only a single encryption and decryption cycle to transmit the information.

In sum respecting claim 5, the novel process is similar to Buffam in that the secure transmission of information at least in part utilizes an encoding key based on the sender's fingerprint. The cited art does not disclose or suggest all of the claimed limitations, and therefore, should not be construed to anticipate the instant invention.

Claims 6-9 involve pre-authentication steps in which the security of the method of transmitting the encoded information is assured to be free from tampering, i.e., the routes of transmission are intrinsically secure. The claims thus explicitly call for authenticating before actually transmitting the encrypted information. Claims 6 and 8 involve respectively authenticating the security of two routes of transmission, specifically a first route of transmission between first party-sender and the key control system, and a second route of transmission between the second party-recipient and the key control system. In contrast according to Buffam, the encoding keys are transmitted in only a single route of transmission, namely, via the transient template. There is no suggestion to authenticate security of the transmission routes by using more than one route of transmission.

Additionally, claims 7 and 9 respectively define steps of returning the encoding keys to the sender and the receiver over the first and second routes of transmission. In Buffam, the encoding key developed from the originator's fingerprint is incorporated with the transmitted information via the transient template. Buffam relies upon the need for the claimant to provide a live fingerprint at the authentication station and the use of plausible imposter false image points mixed with the true fingerprint image points to provide transmission security. These are valuable and no doubt effective techniques but they are different from those of Applicant's claims. Thus there is no prior authentication step disclosed nor is there a step of returning the encoding key to the encoding key generator to verify that the route of transmission is secure from tampering in advance of transmitting the secure information.

It has been shown that the cited reference does not disclose all of the limitations of claims 5-9, and therefore, Applicant urges that the anticipation rejection cannot stand. Claims 10 and 11 depend from these claims and should also be held patentable over the cited reference.

The various differences between Buffam and the novel method may be summarized in the following table.

Buffam US 6,185,316	Kiyomoto 09/766,956	
	Claim	
Enrollee and claimant are same person.	5	Transmits information securely from a first person to a second person
Enrollee provides live fingerprint at enrollment-encryption stage and claimant-putative enrollee provides live fingerprint at authentication-decrypting stage.	5	First person provides one live fingerprint and second person provides one live fingerprint.
Claimant-putative enrollee is present at authentication station to provide second live fingerprint.	5	First and second persons each transmit fingerprint information to independent (i.e., remote) third party key control system.
Encryption key uses plausible imposter false fingerprint image data to disguise true fingerprint image. Protects against theft or loss of transient template held by enrollee.	5	Encryption keys are based on true fingerprint image data. Protection derived from transmission of encryption key separate from encrypted secure data.
Information encrypted once, transmitted with transient template and decrypted once.	5	Information encrypted and decrypted twice. First person encrypts, key controller decrypts and re-encrypts, second person decrypts.
Enrollee carries encrypted information to authentication station.	6	First person (sender) verifies that transmission channel is secure before transmitting encrypted secure information.
Enrollee carries encrypted information to authentication station.	7	Channel of transmission to first person verified by transmitting encryption key to and from third party and comparing returned key to sent key.
Enrollee carries encrypted information to authentication station.	8	Second person (receiver) verifies that transmission channel is secure before transmitting encrypted secure information.
Enrollee carries encrypted information to authentication station.	9	Channel of transmission to second person verified by transmitting encryption key to and from third party and comparing returned key to sent key.

As has been shown, many of the limitations of the claimed invention are not taught or suggested by Buffam. The prior art therefore does not anticipate the claims. For the foregoing reasons, Applicants respectfully request that the rejections be withdrawn and that claims 5-11 be allowed at this time.

Respectfully submitted,

Jeff C Lew

Jeffrey C. Lew
Attorney for Applicant
Registration No. 35,935
Telephone:(302) 475-7919

Date: November 10, 2004
2205 Silverside Road
Wilmington DE 19810
Facsimile:(302) 475-7915